[2345/201]

METHOD AND COMMUNICATIONS DEVICE FOR ELECTRONICALLY SIGNING A MESSAGE IN A MOBILE RADIO TELEPHONE

The present invention is directed to a method for electronically signing a message in a cellular phone, as well as to a communication system specially designed for implementing the method.

In recent times, there has been a significant increase in the electronic transmission of documents, such as application forms and the like. To be able to verify the integrity of the transmitted data and the identity of the originator of the document, methods have been developed for digitally signing messages.

Such a method is known, for example, from the German 197 47 603 T2. In accordance with this method, a message to be signed is first sent from a personal computer via a communications network to a receiving device configured separately from the personal computer. This message is subsequently transmitted from the receiving device via a telephone network to a cellular phone assigned to the transmitting device, the cellular phone being designed as a signing device. The message is signed in the cellular phone by direction of the user and then retransmitted to the receiving device or to another receiver. The known method does, in fact, have the advantage that messages to be signed can be transmitted from a personal computer to a cellular phone functioning as a signing device, without requiring any installations or modifications to be made on the personal computer itself. However, this requires a receiving device that is separate from the personal computer, that transmits the message to be signed to the cellular phone, and that can also receive the signed message back from the cellular phone.

A similar method can also be inferred from the EP 1 027 784.

Thus, the object of the present invention is to provide a method, as well as a communication system for electronically signing a message, which will enable a personal computer to communicate via a communications network directly with a cellular phone as a signing device.

The present invention achieves this objective, first of all, by employing the method steps of Claim 1.

Accordingly, a method is provided for electronically signing a message in a cellular phone. An electronic fingerprint of the message to be signed is first prepared in a personal computer and is subsequently transmitted via a communications network to any cellular phone which contains a signing device. The personal computer may be linked, for example, via an Internet access to the communications network. The received electronic fingerprint is signed in the cellular phone and then retransmitted to the personal computer.

Advantageous embodiments constitute the subject matter of the dependent claims.

To transmit the electronic fingerprint, software is advantageously implemented in the personal computer. It enables the electronic fingerprint to be transmitted via an SMS (short message service), e-mail or WAP (wireless application protocol) service.

The electronic signing may be carried out using any desired cryptographic method, such as the public-key method. To this end, a secret key, which cannot be copied, is first stored in the cellular phone, and a public key, assigned to the secret key, is stored in the personal computer. The public key may be a cryptographic key which is assigned to the owner of the cellular phone. Using the secret key, the cellular phone signs the electronic fingerprint and retransmits it to the

personal computer. The personal computer, in turn, converts the signed electronic fingerprint using the public key into an unencrypted electronic fingerprint. To ascertain that there no manipulation of the transmitted electronic fingerprint has occurred on the unprotected transmission paths of the communications network, the signed electronic fingerprint, that had been converted into an unencrypted electronic fingerprint, is compared to the electronic fingerprint generated from the message to be signed. If the two electronic fingerprints match, it is ensured that no manipulation has taken place on the unprotected transmission paths between the personal computer and the cellular phone.

The electronic fingerprint is preferably generated in accordance with a generally known hash functions, from the message to be signed, and thus represents a specific hash value.

The above named objective is likewise achieved by the features of Claim 5.

Accordingly, a communication system is defined which includes at least one personal computer that is able to be linked to a communications network, as well as at least one cellular phone assigned to the communications network. The personal computer contains a device for generating an electronic fingerprint from a message to be signed, as well as a transmitting device for transmitting the electronic fingerprint to any cellular phone. The cellular phone has a receiving device for receiving an electronic fingerprint transmitted by the personal computer via the communications network, a signing device for signing the received electronic fingerprint, as well as a transmitting device for retransmitting the signed electronic fingerprint to the personal computer.

Advantageous embodiments constitute the subject matter of the dependent claims.

Thus, for example, the cellular phone has a memory for storing a secret key, and the personal computer has a first memory for storing a public key assigned to the secret key. In this manner, the signing of a message may be implemented by using a public-key method. In addition, the personal computer has a device for converting a received, signed electronic fingerprint using the public key, as well as a comparator for comparing the converted electronic fingerprint to the electronic fingerprint generated from the message to be signed.

To be able to transmit the message to be signed, i.e., the electronic fingerprint generated from the message to be signed, from the personal computer to the cellular phone, and to be able to receive it again from the same, special communications software is to be implemented in the personal computer. This software may be stored in another memory.

In one practical embodiment, the personal computer has a third memory in which at least the call number of the cellular phone is stored that the personal computer automatically dials when a message to be signed is to be signed by a cellular phone. The call numbers of other cellular phones or other signing devices that are reachable via the communications network, as well as the call number or call numbers of specific target devices may likewise be stored in the third memory.

The present invention is elucidated in the following on the basis of an exemplary embodiment, with reference to the enclosed drawing.

The only figure shows a personal computer 10, which may be linked via a communications network 110, for example a cellular network, to a cellular phone, also referred to, in short, as cell phone 60. Using the exemplary communication system, a document created at personal computer 10 may be

sent via communications network 110 to an addressee, in the following also called target device 100.

For this purpose, personal computer 10 has a generally known transmitting/receiving device 20, via which personal computer 10 is linked to communications network 110. In a memory 30, one or more call numbers may be stored, which, in the present example, belong to cell phone 60 and to target device 100, to which a signed document is to be sent. To be able to sign or encrypt a document, for example in accordance with the public-key method, as explained in greater detail further below, a so-called public key, which belongs to the owner of cell phone 60 and which is available to the public, is able to be stored in another memory 32. A document to be signed that has been created at personal computer 10, may be stored in a memory 34. Typically, however, it is not the completed document that is signed, but rather only an electronic fingerprint generated from the completed document. Such an electronic fingerprint may be calculated from the completed document, using a hash function, for example. The calculated value, also referred to as hash value, may be stored in a memory 36. To enable personal computer 10 to communicate via communications network 110 with cell phone 60, a suitable communications software is stored in a memory 38. The control of personal computer 10, the calculation of an electronic fingerprint from a completed document, and the decryption of an electronic fingerprint signed by cell phone 60 may take place in decentrally located devices or in a central control unit 40, as shown in the figure. Control unit 40 communicates with memories 30, 32, 34, 36 and 38, as well as with transmitting/receiving device 20.

Besides a transmitting/receiving device 70, known per se, and an antenna 120, cell phone 60, which is provided with a signing function, has a signing device 90, which is linked to a memory 80, in which a secret key, in particular the secret key of the owner of cell phone 60 is stored.

The method of functioning of the communication system illustrated in the figure is explained in greater detail in the following.

It is assumed here that a document created at personal computer 10, for example a purchase contract in signed form, is to be transmitted to target device 100. The document previously stored in document memory 34 is read out by control unit 40. Then, with the aid of a hash function, control unit 40 generates an electronic fingerprint from the document. This electronic fingerprint may be designated as the hash value. This hash value is stored in memory 36. Via a keyboard of personal computer 10, the user may now initiate the process of signing the requested document. To this end, a connection set-up to cell phone 60 is automatically initiated via communications network 110 in that the call number of cell phone 60 stored in memory 30 is read out and supplied to communications network 110 to be evaluated accordingly. Or, if there is a plurality of cell phones having the signing feature, the user himself/herself may also enter the call number of the cell phone in question via the keyboard of personal computer 10. The hash value stored in memory 36 is subsequently transmitted via transmitting/receiving device 20 of personal computer 10 via the communications network to cell phone 60. It is noted at this point that the transmission paths via communications network 110 are unprotected. Via transmitting/receiving device 70 of cell phone 60, the received hash value attains signing device 90. Signing device 90 and memory 80 may be permanently implemented in the cell phone or constitute part of a chip card which is insertable into the cell phone. To sign the received hash value, signing device 90 reads the secret key from memory 80 and encrypts or signs the hash value in accordance with the public-key method. The signed hash value is subsequently retransmitted via transmitting/receiving device 70 and antenna 120 that is schematically depicted in the figure, via communications network 110, directly back to personal computer 10. Via transmitting/receiving device 20, the signed hash value

attains control unit 40, which, using the public key stored in memory 32, decrypts the signed hash value, i.e., reconverts it to the unencrypted hash value again. The decrypted hash value is then fed, together with the hash value that is stored in memory 36 and directly generated from the completed document, to comparator 50 and compared in this device. If the hash value stored in memory 36 and the decrypted hash value match, then no manipulation has taken place on the unprotected transmission paths of communications network 110 between personal computer 10 and cell phone 60. Thus, the document stored in memory 34, including the hash value stored in memory 36, is effectively signed; it may now be transmitted to addressee 100.

For this, a separate automatic dialer or control unit 40 reads the corresponding call number (or e-mail address, etc.) of target device 100 from memory 30 and establishes a connection to this number, provided that the addressee is connected to communications network 110. Finally, the signed document is transmitted to target device 100.

Reference Symbol List

10 personal computer

20 transmitting/receiving device of the personal computer

30 memory for at least one cell phone call number

32 memory for a public key

34 memory for a document to be signed

36 memory for a hash value

38 memory for communications software

40 control unit

50 comparator

60 cell phone

70 transmitting/receiving device

80 memory for a secret key

90 signing device

100 target device

110 communications network, in particular cellular network